IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Wallman	**Conf. No.**:	1382
Serial No.:	10/667,852	**Art Unit**:	2434
Filed:	9/22/2003	**Examiner**:	Tolentino, R.
Title:	**SYSTEM AND METHOD FOR PROVIDING PHYSICAL WEB SECURITY USING IP ADDRESSES**	**Docket No.**:	CHA920030022US1 (IBMC-0076)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANT

This is an appeal from the Final Rejection dated August 21, 2008 and the Advisory Action of October 23, 2008, rejecting claims 1, 3-11 and 13-16. This Brief is accompanied by the requisite fee set forth in 37 C.F.R. 1.17 (c).

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

As filed, this case included claims 1-16. Claims 1, 3-11 and 13-16 remain pending, stand rejected, and form the basis of this appeal. Claims 2 and 12 have been cancelled.

STATUS OF AMENDMENTS

An After-Final Response, filed on October 15, 2008 in response to the Final Action dated August 21, 2008, did not result in the allowance of the claims.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides a system for providing security for an internet server (independent claim 1), a method for authenticating a user accessing an Internet server (independent claim 7) and a program product for providing security for an Internet server (independent claim 11).

The system for providing security for an Internet server (independent claim 1) includes: a logical security system (e.g., Logical Security System 14, FIG. 1; page 4, line 11) for processing login and password data (e.g., Initial Security Info 28, FIG. 1; page 5, line 1) received from a client device (e.g., CLIENT DEVICE 24, FIG. 1; page 4, line 23-page 5, line 1) during a server session with the Internet server (e.g., SERVER 10, FIG. 1; page 4, line 16) in order to authenticate a user (e.g., USER 20, FIG. 1; page 4, line 16); a physical security system (e.g., Physical Security System 16, FIG. 1; page 4, lines 11-12) for processing Internet protocol (IP) address information (e.g., IP Address 26, FIG. 1; page 5, line 5) of the client device at the Internet server in order to authenticate the client device for the duration of the server session; and a memory system (e.g., Memory System 13, FIG. 1; page 4, line 14) for storing, at the Internet

server, a list of each logged in user and a reference IP address (e.g., IP Address 26, FIG. 1; page 5, line 5) collected during a login procedure.

The method for authenticating a user accessing an Internet server (independent claim 7) includes: storing in a memory system (e.g., Memory System 13, FIG. 1; page 4, line 14), at the Internet server (e.g., SERVER 10, FIG. 1; page 4, line 16), a reference Internet protocol (IP) address (e.g., IP Address 26, FIG. 1; page 5, line 5) and associated login data (e.g., Initial Security Info 28, FIG. 1; page 5, line 1) whenever a new server session is initiated on the Internet server from a client device (e.g., CLIENT DEVICE 24, FIG. 1; page 4, line 23-page 5, line 1); receiving a message (e.g., Messages 29, FIG. 1; page 5, line 16) from a requesting user (e.g., USER 20, FIG. 1; page 4, line 16) at the Internet server; obtaining login data (e.g., Initial Security Info 28, FIG. 1; page 5, line 1) accompanying the message; obtaining an IP address (e.g., IP Address 26, FIG. 1; page 5, line 5) from a message header in the message; determining if the login data of the requesting user is currently listed in the memory system as an existing session with the Internet server; and if the login data of the requesting user is currently listed, determining at the Internet server if the IP address from the received message matches the reference IP address associated with the login data of the requesting user.

The program product for providing security for an Internet server (independent claim 11) includes: means for (e.g., Logical Security System 14, FIG. 1; page 4, line 11) processing logical security information (e.g., Initial Security Info 28, FIG. 1; page 5, line 1) received from a client device (e.g., CLIENT DEVICE 24, FIG. 1; page 4, line 23-page 5, line 1) during a server (e.g., SERVER 10, FIG. 1; page 4, line 16) session in order to authenticate a user (e.g., USER 20, FIG. 1; page 4, line 16); means for (e.g., Physical Security System 16, FIG. 1; page 4, lines 11-12) processing Internet protocol (IP) address information (e.g., IP Address 26, FIG. 1; page 5, line 5)

of the client device in order to authenticate the client device during the server session by comparing the IP address of a received message (e.g., Messages 29, FIG. 1; page 5, line 16) against the list of IP addresses stored by the server; and means for storing, at the Internet server, a list of each logged in user and a respective reference IP address (e.g., IP Address 26, FIG. 1; page 5, line 5) collected during a login procedure.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(1) Whether claims 1, 3-4 and 6-10 are unpatentable under 35 U.S.C. 103(a) over Sasmazel et al. (U.S. Patent No. 6,725,376), hereafter "Sasmazel" in view of Limisco (U.S. Patent No. 6,662,228), hereafter "Limisco."

(2) Whether claims 11, 13-14 and 16 are unpatentable under 35 U.S.C. 103(a) over Sasmazel in view of Limisco, and in further view of Clark et al. (U.S. Patent No. 6,442,588), hereafter "Clark."

(3) Whether claim 5 is unpatentable under 35 U.S.C. 103(a) over Sasmazel in view of Limisco, and in further view of Muratov et al. (U.S. PG-Pub. No. 2003/0097596), hereafter "Muratov."

(4) Whether claim 15 is unpatentable under 35 U.S.C. 103(a) over Sasmazel in view of Limisco, in further view of Clark, and in further view of Muratov.

ARGUMENT

(1) Rejection of claims 1, 3-4 and 6-10 over Sasmazel and Limisco under 35 U.S.C. 103(a).

The rejection under 35 U.S.C. 103(a) is defective because the references Sasmazel and Limisco, taken alone or in combination, fail to disclose or suggest each and every feature of the claims.

Independent claim 1 reads in part, "...a memory system for storing, at the Internet server, a list of each logged in user and a reference IP address collected during a login procedure..." (Claim 1, and similarly recited in claims 7 and 11). In its Final Rejection, the Office posits that Sasmazel discloses a memory system for storing a list of each logged in user and a reference IP address collected during a login procedure. (Final Rejection at page 4; Sasmazel at cl. 4). However, Sasmazel fails, *inter alia*, to disclose the above-referenced features of claim 1. At best, Sasmazel discloses using an "eticket" generated by an authentication server and passed from server to server to avoid the need for "reauthentication." (Sasmazel at col. 7, line 59-col. 9, line 3). While the "eticket" of Sasmazel is disclosed as including a "ticket framework" containing a client IP address, the client IP address is neither stored at the Internet server, nor is it contained in a list. (*Id.*). Therefore, Sasmazel does not disclose storing a list of each logged in user and a reference IP address collected during a login procedure.

Further, claim 1 also reads in part, "...a physical security system for processing Internet protocol (IP) address information of the client device at the Internet server... and a memory system for storing, at the Internet server, a list..." (Claim 1, and similarly recited in claims 7 and 11). In the Advisory Action of 23 October 2008, the Office argues that "[a]n authentication server used for verifying users, will have a list of acceptable users..." (Advisory Action at page

2). However, Appellant respectfully submits that the Office discounts the effect of the isolated authentication server of Sasmazel. In contrast to Sasmazel, claim 1 is drawn to a system comprising, *inter alia*, a physical security system and a memory system, both of which are located at the Internet server. Sasmazel, however, discloses a separate authentication server which creates an "eticket" and passes it to other servers for later access by users. (*Id.*; See above discussion). In isolating the authentication server, Sasmazel necessarily fails to disclose, *inter alia*, a "physical security system …at the Internet server…," and further fails to disclose "…a memory system for storing a list of each logged in user and a reference IP address collected during a login procedure…" located at the same server. (Claim 1)(Emphasis added).

Limisco fails to overcome the deficiencies of Sasmazel, addressed above.

(2) Rejection of claims 11, 13-14 and 16 over Sasmazel, Limisco and Clark under 35 U.S.C. 103(a).

The rejection under 35 U.S.C. 103(a) is defective because the references Sasmazel, Limisco and Clark, taken alone or in combination, fail to disclose or suggest each and every feature of the claims.

Regarding independent claim 11, Appellant hereby incorporates the arguments made with respect to similarly recited independent claim 1. Clark fails to overcome the deficiencies of Sasmazel and Limisco, addressed above. (See Item No. 1).

Appellant further requests the Office's assistance in amending claims 13 and 16 from "[t]he program product of claim 12" to read in part, "[t]he program product of claim 11." Appellant inadvertently submitted the Amendment of 15 October 2008 without amending these references to cancelled claim 12. However, Appellant asserts that in viewing the file, the Office

will find that claims 13 and 16 are properly dependent upon claim 11, as claim 11 contains subject matter previously contained in cancelled claim 12. As such, Appellant respectfully requests the Office's assistance in this matter.

(3) Rejection of claim 5 is over Sasmazel, Limisco, and Muratov under 35 U.S.C. 103(a).

The rejection under 35 U.S.C. 103(a) is defective because the references Sasmazel, Limisco and Muratov, taken alone or in combination, fail to disclose or suggest each and every feature of the claims.

Regarding dependent claim 5, Appellant hereby incorporates the arguments made with respect to independent claim 1, from which claim 5 depends. Muratov fails to overcome the deficiencies of Sasmazel and Limisco, addressed above. (See Item No. 1).

(4) Rejection of claim 15 is over Sasmazel, Limisco, Clark and Muratov under 35 U.S.C. 103(a).

The rejection under 35 U.S.C. 103(a) is defective because the references Sasmazel, Limisco, Clark and Muratov, taken alone or in combination, fail to disclose or suggest each and every feature of the claims.

Regarding dependent claim 15, Appellant hereby incorporates the arguments made with respect to independent claim 11, from which claim 15 depends. Muratov fails to overcome the deficiencies of Sasmazel, Limisco and Clark, addressed above. (See Item No. 2).

Accordingly, Appellant submits that all pending claims are allowable because Sasmazel, Limisco, Clark and Muratov, taken alone or in combination, fail to disclose or suggest each and every feature of the claims as required by 35 U.S.C. 103(a).

Respectfully submitted,

/Matthew B. Pinckney/

Matthew B. Pinckney
Reg. No. 62,727

Date: 9 February 2009

Hoffman Warnick, LLC
75 State Street, 14th Floor
Albany, New York 12207
Phone: (518) 449-0044
Fax: (518) 449-0047

CLAIMS APPENDIX

1. A system for providing security for an Internet server, comprising:

a logical security system for processing login and password data received from a client device during a server session with the Internet server in order to authenticate a user;

a physical security system for processing Internet protocol (IP) address information of the client device at the Internet server in order to authenticate the client device for the duration of the server session; and

a memory system for storing, at the Internet server, a list of each logged in user and a reference IP address collected during a login procedure.

3. The system of claim 2, wherein the physical security system compares the IP address of a received message with the reference IP address for the user.

4. The system of claim 3, wherein the physical security system terminates the session for the user if the IP address obtained from the received message does not match the reference IP address for the logged in user.

5. The system of claim 4, wherein the physical security system deletes all instances of the logged in user from the stored list if the IP address obtained from the received message does not match the reference IP address for the logged in user.

6. The system of claim 2, wherein the physical security system includes a proxy server module for comparing a portion of an IP address obtained from a received message against a like portion of the reference IP address for the logged in user.

7. A method of authenticating a user accessing an Internet server, comprising:

storing in a memory system, at the Internet server, a reference Internet protocol (IP) address and associated login data whenever a new server session is initiated on the Internet server from a client device;

receiving a message from a requesting user at the Internet server;

obtaining login data accompanying the message;

obtaining an IP address from a message header in the message;

determining if the login data of the requesting user is currently listed in the memory system as an existing session with the Internet server; and

if the login data of the requesting user is currently listed, determining at the Internet server if the IP address from the received message matches the reference IP address associated with the login data of the requesting user.

8. The method of claim 7, comprising the further step of initiating a login procedure if the login data of the requesting user is not currently listed in the memory system.

9. The method of claim 7, comprising the further step of terminating all server sessions listed in the memory system having the login data of the requesting user if the IP address from the obtained message does not match the reference IP address.

10. The method of claim 7, wherein the step of determining if the IP address from the received message matches the reference IP address associated with the login data of the requesting user includes the steps of:

examining a portion of the IP address of the requesting user; and

determining if the portion matches a like portion of the reference IP address.

11. A program product stored on a recordable medium for providing security for an Internet server, the program product comprising:

means for processing logical security information received from a client device during a server session in order to authenticate a user;

means for processing Internet protocol (IP) address information of the client device in order to authenticate the client device during the server session by comparing the IP address of a received message against the list of IP addresses stored by the server; and

means for storing, at the Internet server, a list of each logged in user and a respective reference IP address collected during a login procedure.

13. The program product of claim 12, wherein the means for processing IP address information compares a login name and IP address of a received message against the list of logged in users and their respective reference IP addresses.

14. The program product of claim 13, wherein the means for processing IP address information terminates the session for the user if the IP address obtained from the received message does not match the reference IP address for the logged in user stored in the list.

15. The program product of claim 14, wherein the means for processing IP address information deletes all instances of the logged in user from the stored list if the IP address obtained from the received message does not match the respective reference IP address for the logged in user.

16. The program product of claim 12, wherein the wherein the means for processing IP address information includes a proxy server module for comparing a portion of an IP address obtained from a received message against a like portion of the reference IP address for the logged in user.

EVIDENCE APPENDIX

No evidence has been submitted.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.